PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) **Classification internationale des brevets** 7 : **H04L 9/06** — **A1**

(11) **Numéro de publication internationale:** **WO 00/54454**

(43) **Date de publication internationale:** 14 septembre 2000 (14.09.00)

(21) **Numéro de la demande internationale:** PCT/FR00/00283

(22) **Date de dépôt international:** 7 février 2000 (07.02.00)

(30) **Données relatives à la priorité:**
99/02834 8 mars 1999 (08.03.99) FR

(71) **Déposant** *(pour tous les Etats désignés sauf US)*: GEMPLUS [FR/FR]; Avenue du Pic de Bertagne, Parc d'activités de Gèmenos, F–13881 Gèmenos (FR).

(72) **Inventeur; et**
(75) **Inventeur/Déposant** *(US seulement)*: BENOIT, Olivier [FR/FR]; La Treille d'Azur Bât. D, F–13400 Aubagne (FR).

(74) **Mandataire:** NONNENMACHER, Bernard; Avenue du Pic de Bertagne, Parc d'activités de Gèmenos, F–13881 Gèmenos (FR).

(81) **Etats désignés:** AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée
Avec rapport de recherche internationale.

(54) **Title:** COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT USING A SECRET KEY CRYPTOGRAPHIC ALGORITHM

(54) **Titre:** PROCEDE DE CONTRE–MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE SECRETE

(57) **Abstract**

In an electronic component using a secret key cryptographic algorithm K whereof the operation comprising several successive computing cycles T1, T16 to supply from initial input data L0, R0 applied at the first cycle, final output data L16, R16 at the last cycle, the method consists in applying a first random value u to the computing means designed for each cycle (TC_M) to obtain in output unpredictable data ($a \oplus u$). The invention is characterised in that it consists further in applying a second random value v to said initial input data L0 and R0 applied in input of the first cycle T1.

(57) **Abrégé**

Dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète K, dont la mise en oeuvre comprenant plusieurs tours de calculs successifs T1, T16 pour fournir à partir des premières données d'entrées L0, R0 appliquées au premier tour T1, des données finales L16, R16 en sortie du dernier tour T16, on applique une première valeur aléatoire u à des moyens de calculs prévus dans chaque tour (TC_M) pour obtenir en sortie des données imprédictibles ($a \oplus u$). Selon l'invention on applique en outre une deuxième valeur aléatoire v auxdites premières données d'entrée L0 et R0 appliquées en entrée du premier tour T1.